

NISCC Vulnerability Advisory 482323/NISCC/ADOBE

Vulnerability Issues with Adobe Reader

Version Information

Advisory Reference	482323/NISCC/ADOBE
Release Date	1 April 2005
Last Revision	5 April 2005
Version Number	1.1

What is Affected?

The Windows version of:

- Adobe Reader v7.0 and earlier
- Adobe Acrobat v7.0 and earlier

Impact

If exploited it may be possible to discover the existence of local files on an end-user system.

Severity

This is rated as low.

Summary

A vulnerability within the Adobe Reader control have been identified; under certain circumstances if the control is placed on a web page, it is possible to discover the existence of local files by monitoring the behaviour of certain methods.

Adobe has solutions available that can rectify these issues; please refer to the 'Solution' section for further information.

Details

CVE ID: CAN-2005-0035

The vulnerability is within the Adobe Reader control; if the control is placed on a web page, it is possible to discover the existence of local files by calling the `.LoadFile(filename)` method and monitoring its behaviour.

An attacker could then use the information gathered to help prepare for a more serious attack.

However the impact is minimised due to the fact that the existence of local files can only be discovered if the complete filenames and paths are known in advance by the attacker.

Mitigation

Upgrade to the latest stable version of the Adobe Reader and Adobe Acrobat software.

Solution

Adobe recommends the following:

- If you are using Adobe Reader, then upgrade to Adobe Reader v7.0.1
- If you are using Adobe Acrobat, then upgrade to Adobe Acrobat v7.0.1

Vendor Information

Adobe is headquartered in San Jose, California and was founded in 1982. For further information, please visit their website at <http://www.adobe.com/>.

Acknowledgements

The NISCC Vulnerability Team would like to thank CESG for reporting the issue to us and Adobe for their co-operation with the handling of this vulnerability.

Contact Information

The NISCC Vulnerability Management Team can be contacted as follows:

Email	vulteam@nisc.gov.uk <i>(Please quote the advisory reference in the subject line.)</i>
Telephone	+44 (0)870 487 0748 Extension 4511 <i>(Monday to Friday 08:30 - 17:00)</i>
Fax	+44 (0)870 487 0749

Post	Vulnerability Management Team NISCC PO Box 832 London SW1P 1BG
------	--

We encourage those who wish to communicate via email to make use of our PGP key. This is available from <http://www.niscc.gov.uk/niscc/publicKey2-en.pop>.

Please note that UK government protectively marked material should not be sent to the email address above.

If you wish to be added to our email distribution list, please email your request to uniras@niscc.gov.uk.

What is NISCC?

For further information regarding the UK National Infrastructure Security Co-Ordination Centre, please visit the NISCC web site at: <http://www.niscc.gov.uk/>

Reference to any specific commercial product, process or service by trade name, trademark manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

Neither shall NISCC accept responsibility for any errors or omissions contained within this advisory. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

© 2005 Crown Copyright

Revision History

1 April 2005	Initial release (1.0)
5 April 2005	Amended details (1.1)

<End of NISCC Vulnerability Advisory>